

Seth Aikens

Defendant's Response to Government's Proposed Findings of Facts & Conclusions of Law

Dear Honorable Judge Hardy:

I, Seth Allen Aikens II, declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the following statements are true and correct.

I hereby incorporate the entire record in this case, including all exhibits, transcripts, motions, briefs, arguments, filings, and other materials the Court may consider.

I respectfully submit this response to assist the Court by providing technical demonstrations and clarifications regarding encryption systems, a detailed explanation of the trail camera and associated lighting, as well as an account of evidence handling and relevant Governmental meeting procedures. These clarifications address gaps or ambiguities in the present record.

Exhibits 131.1 through 132.7 are playable videos of the projects. Exhibit 132.4 contains the "Ryan and Erick Trail Cam & Light Talk.mp4," and Exhibit 131.12 demonstrates the MacBook missing a hard drive, corroborated by Exhibit 74, which further establishes the authenticity of these claims. Exhibit 131.9 includes a video explainer "Encryption Explainer.mp4" with custom software I developed to illustrate/emulate/showcase etc the encryption process. Additionally, Exhibits 1, 2, and 3 directly rebut the Government's E01 claims in furtherance of Page 14 Section X herein.

I. DEFENDANT'S DECLARATION AND STANDING

I am the defendant in this matter and submit this declaration based upon my personal knowledge and direct experience with the systems, evidence, and procedures described herein.

II. TECHNICAL DEMONSTRATIONS PROVIDED TO THE COURT

A. Trail Camera Demonstration and Technical Foundation

Seth Aikens

To assist the Court's understanding of the technical aspects of this case, I have prepared a comprehensive video demonstration that illustrates the complete functionality of a trail camera system. This demonstration provides a detailed breakdown of how trail cameras, camera viewing, image burning, modeling, the mobile application, and associated lighting systems operate in practice, including a complete trail camera simulation demonstrating streaming capabilities and interconnected components.

In this video, I also touch on Erick Merryman's lights. (He was friends with Ryan) so some technology such as socket delivery etc is the same.

This demonstration directly addresses Your Honor's previous observation that individuals should typically remember systems or evidence they have operated or possessed, providing substantial technical foundation supporting my testimony regarding familiarity with these systems. (Noted In Miah)

B. Encryption and Password Security Demonstration

I have prepared a second video demonstration specifically addressing the encryption methods relevant to this case. This video illustrates how encryption can be decrypted when proper passwords are available, and demonstrates how straightforward it would have been for Government investigators to access encrypted materials without requiring my assistance in entering passwords.

I developed a custom software tool specifically for this Court's review, in response to Government allegations suggesting I lack technical knowledge in this area. The demonstration covers creation of two different types of encrypted containers, including detailed procedures for mounting and unmounting volumes, locking and unlocking containers, and adding and removing files from encrypted storage. It clearly shows the Government **never needed my physical help**.

III. CIRCUMSTANCES OF SEIZURE AND INITIAL SYSTEM STATE

A. Computer System Already Logged In

Seth Aikens

At the time of the warrant's execution and seizure, the primary computer system was already logged into the operating system with the encryption key, providing complete access to all available data, applications, and files. Simple lock password that is 3 digits next to the encryption key on the now missing papers listing passwords as stated in the prior findings of facts, Agent Coleman clearly articulated these missing papers if he felt confident shutting this off.

B. Credentials Available on Papers at Time of Seizure

At the time of the seizure, all passwords and system credentials were clearly documented in physical form--written on papers that were both present and readily available. These documents were systematically organized and stored in a manner that made them easily accessible. During the evidence collection process, Government agents located and seized these credential documents as part of their procedures.

It is important to emphasize that the exhibits themselves clearly show that these documents were taken by the agents. In fact, in other exhibits, it is evident that the agents seized not only my credential papers but also personal documents such as my child's birth certificate (Which they still haven't returned). One of the exhibits even depicts the birth certificate lying on the desk. (Picture with Agent Fell & I), further confirming their handling and presence of these materials during the search.

Additionally, the evidence makes it clear that a USB drive was also seized. (The binder was taken) This USB was stored in the silver binder along with the credential documents.

Regardless of any claims made by the agents regarding how they obtained these credentials, none of the photographs or exhibits in evidence support their assertions about the source or location of these documents. Instead, the evidence reinforces my account: I have direct and personal knowledge of where I stored my materials, and I am confident the documents--including the papers, the USB drive in the silver binder is precisely where I left them at the time of the seizure.

Seth Aikens

Therefore, any suggestion that the credentials or other items were obtained from a source other than the physical items seized is not supported by the available evidence. The documentation and the circumstances of their discovery are clear and verifiable, and no photographic or documentary evidence has been presented that contradicts my account. Furthermore to that, I've attached the entire search warrant log and photos of rooms related before & after.

C. RAM Dump Capability at Time of Seizure

Given that the system was already logged in and operational at the time of seizure, a complete RAM (Random Access Memory) dump was entirely possible and would have provided immediate access to:

- Currently loaded encryption keys & data in active memory
- Complete image where we could extract the actual password database

This technical capability represents standard forensic procedure that could have bypassed encryption barriers without requiring any additional passwords or cooperation from me. (The DOJ Forensic Guide specifically cautions people when powering off devices)

D. USB Device Present at Time of Seizure

There was a USB storage device present at the time of seizure that contained additional relevant data. This USB device has since gone missing from the Government's control and custody and represents missing evidence that should be accounted for in the Government's evidence preservation protocols. This device was with the papers in the silver binder.

IV. PASSWORD KNOWLEDGE AND SECURITY SYSTEMS

A. Password Storage and Organization

I do not possess or maintain any substantive knowledge of the passwords pertinent to this matter, aside from an awareness of their physical storage location. All passwords under my custody were carefully recorded and systematically maintained within a silver binder consisting of thirty-one

Seth Aikens

(31) pages. At all times when not in active use, this binder was securely stored in a safe to ensure its protection.

The passwords documented within this binder were thoroughly organized and accompanied by precise identifying details, which included:

- **Computer names and system identifiers:** Each password entry was linked to the specific device or system it pertained to.
- **Container names and volume designations:** For passwords related to encrypted containers or virtual drives, the relevant names and identifiers were clearly noted.
- **Drive letters and storage device identifiers:** Where applicable, the corresponding drive letter or storage device was specified for clarity.
- **Cloud-based accounts:** Entries for cloud services included the associated email address, corresponding password, and, where applicable, any two-factor authentication (2FA) codes necessary for access.

This methodical approach ensured that all credentials were both accessible for authorized use and protected against unauthorized disclosure.

B. Password Complexity and Non-Constructive Nature

The passwords recorded in the binder were generated using cryptographically secure, random methods. Because of their randomly generated, non-constructive nature, it is mathematically infeasible to memorize or reconstruct these passwords through recall alone.

These passwords are generated non-constructive, meaning they do not contain recognizable words, personal information, or identifiable patterns. As a result, they are highly resistant to common attack vectors, including brute-force attacks, dictionary attacks, and data analysis techniques. The generation process used cryptographically secure random number and character generators to eliminate any possibility of predictability or pattern recognition.

Seth Aikens

Concerns that such passwords could be reconstructed or guessed, as has been suggested, are unfounded. The passwords do not rely on any personal references or dictionary-based elements that could be exploited by an attacker. Furthermore, the defenses have reviewed other digital passwords in electronic discovery, none of those are relevant to this matter, as the passwords in question are exclusively located in the three specified locations: the binder, a USB drive, or the logged In PC (RamDump or Normal Image with papers listing passwords now gone)

In summary, the security measures and password generation methods employed make it virtually impossible for anyone to reconstruct or memorize these passwords outside of their documented storage.

V. Government MEETING AND ATTEMPTED DEVICE ACCESS

A. Meeting Timeline and Logistics

The Government-arranged meeting was conducted with law enforcement agents already present at the facility upon my arrival. I arrived approximately 45 minutes early for the scheduled meeting. The Assistant United States Attorney (AUSA) arrived approximately 25 minutes after my arrival, with Frank arriving precisely on time.

Upon entry to the federal facility, we underwent standard security screening procedures, waited for Agent Fell's arrival, proceeded upstairs via elevator, and entered a room containing the computers, books, documents, and other evidentiary objects as documented in the photographic record.

B. Initial Device Access Attempts

The first directive to law enforcement was to demonstrate that the MacBook was functioning and to observe its request for an encryption key upon startup. Agent Coleman retrieved a charger for the device, connected it, and initiated the boot sequence. The device displayed that it could not complete the boot. Nothing todo with encryption.

C. Password Presentation and My Response

Seth Aikens

Government representatives presented various passwords and the AUSA inquired whether I would attempt to use any of them to access the encrypted systems. My response was unequivocal: **"NOT UNLESS YOU HAVE THE PASSWORDS"** - emphasizing that the passwords being presented were not the correct ones for the containers in question.

The passwords presented represented materials seized from my residence, some dating back to 2017 and 2018 accounts, demonstrating my long-standing practice of maintaining comprehensive password records since residing at both 725 South 5th Avenue, Clarion, and 60 Rocky Grove Lane, Crown, Pennsylvania.

D. Response to AUSA's Forensic Training Inquiry

When the AUSA asked about my forensic training, I referenced my work with the bodycam app as an example. To properly analyze mobile applications, you inevitably need to use forensic tools and methodologies. This isn't just casual software review - it requires understanding file systems, data structures, memory allocation, and how applications store and process information.

Given my extensive background with operating systems and software architecture, I've necessarily developed familiarity with forensic procedures and tools over the years. When you're working at the system level, troubleshooting software issues, or analyzing how applications function, you're essentially using the same investigative approaches that formal forensic analysis employs. You're examining logs, tracing data flows, understanding how information is stored and retrieved, and reconstructing sequences of events based on digital evidence.

This extends even down to the databases these applications use. Take something like a message anomaly - to understand its core, you need to comprehend how messaging systems store data, the database schemas they employ, and how different message states are tracked. For instance, Apple's Messages app uses specific database structures and protocols that are well-documented in technical resources like The Apple Wiki, which details everything from message storage formats to delivery mechanisms and synchronization processes (<https://theapplewiki.com/wiki/Messages> Last Visited Aug 5th 2025)

Seth Aikens

My experience includes understanding how mobile and desktop aswell as other operating systems handle data, how applications interact with system resources, how databases are structured and queried, and how to trace the digital footprints that software leaves behind. Whether you're analyzing why a message failed to deliver, investigating data corruption, or examining application behavior, you're working with the same database forensics principles - understanding schema design, transaction logs, data integrity, and how information flows through interconnected systems.

Whether you call it troubleshooting, reverse engineering, or forensic analysis, the underlying technical skills and investigative mindset are fundamentally the same. The tools I've used for legitimate software analysis - debuggers, hex editors, file system analyzers, network monitors, database browsers - are the same categories of tools used in digital forensics.

So while I may not have formal certification in forensic procedures, my years of hands-on technical work have given me practical experience with the same investigative techniques and analytical tools that forensic specialists use. None the less hundreds of people use my apps.

E. Agent Coleman's Technical Preparations and Fundamental Failures

According to Exhibit 18, Agent Coleman brought two specific software tools: FTK Imager and TrueCrypt. This raises serious concerns about the Government's technical competence.

Critical Technical Issue: TrueCrypt Demonstrates No Prior Review

Agent Coleman's preparation with TrueCrypt software definitively demonstrates that he never actually reviewed or examined the encryption systems on the seized devices. TrueCrypt ceased being supported many years ago and is not compatible with VeraCrypt, the current standard encryption software. (Last Visited Aug 5th 2025 <https://en.wikipedia.org/wiki/TrueCrypt> 7.2 / May 28, 2014; 11 years ago (Discontinued))

The encryption systems in question utilize Cryptomator for cloud-based encryption and VeraCrypt for local encryption - not obsolete TrueCrypt. Agent Coleman's use of TrueCrypt tools

Seth Aikens

is not a matter of using a "wrong tool that can break it" - rather, it conclusively proves he never conducted any preliminary forensic examination to identify what encryption software was actually in use.

Any competent forensic examiner would have immediately identified the encryption types through basic file system analysis, header examination, or simple observations.

VI. EVIDENCE CORRUPTION AND FORENSIC FAILURES

A. Time-Related Corruption and Storage Issues

I have attached exhibits 5 through 17 illustrating several instances where encrypted volumes have become corrupted over time for no reasons even. Digital storage devices (Cloud servers use hardware too...) are inherently vulnerable to degradation and corruption, especially when stored for long periods without appropriate maintenance or when handled improperly.

The elapsed time between the initial seizure and the present review may have contributed to significant corruption of the encrypted containers and file systems. Without immediate and proper forensic preservation at the time of seizure, it is impossible to reliably assess the current condition of these devices. Furthermore, it was represented to a federal judge--and repeatedly confirmed by the US Attorney--that the devices would be imaged offsite and the forensic reviews had been underway. (Reference the Warrant)

Simply noting the US Attorney hasn't let us review the 2 black drives, therefore, we don't know any further details nor health.

B. Complete Absence of Forensic Images

The Government has not produced any forensic images, representing a fundamental failure in digital evidence preservation. Standard forensic protocol requires timely creation of bit-for-bit forensic images upon seizure to preserve evidence integrity and prevent corruption. Where did Rule 41 go? Soeka doesn't get our challenge, the Government faked evidence files while they

Seth Aikens

could have been doing a real exam they represented twice they'd been doing. They physically went out of there way to mark not just 1 or 2 files, but a good multiple.

Critical Missing Forensic Evidence:

1. **Where is the USB image?** No forensic image of the USB device present at seizure has been created or produced, and the device itself is now missing from Government inventory.
2. **Where is the MacBook image, harddrive?** No forensic image of the MacBook has been created or produced, despite this being central evidence.
3. **Where are the 2 drive images that contain the containers?** The two black drives specifically requested in our motion weren't even allowed to be powered on during the meeting. These black drives contain backups of all.

C. Government's Undisclosed "Cracking Process"

The Government has not revealed their alleged "cracking process" or methodology. This lack of transparency raises serious questions about their actual procedures and potential damage to evidence.

Write Blocker Claims Without Proof

While the Government may claim they used write blockers during their examination procedures, they have provided no documentation, logs, or verification that write blockers were actually utilized (Other than our meeting). Simply claiming the use of write blockers does not constitute proof that proper forensic protocols were followed. (No new chain of custody filled during our meeting?)

Without documented proof of write blocker usage, chain of custody documentation, and forensic imaging procedures, there is no way to verify that evidence integrity has been maintained or that the Government's examination processes have not damaged critical files or encryption structures.

VII. Government REFUSAL TO CONDUCT PROPER EXAMINATION

Seth Aikens

A. Scope of Access Request and Preparation Failures

Throughout the hearing and legal briefings, we clearly specified that our request for access was for two black drives, and that the other device statuses were materially misrepresented for encrypted/non encrypted, as the exhibits here show. It was only after the AUSA admitted he had not reviewed the record for my list of spoiled items that he began asking and probing about other devices and my recollections, what files are where etc. Our motion has always been narrowly tailored and explicit. We addressed each issue as it arose--first, the ram dump; then, the passwords--with both sides responding accordingly. (If we can access full backups, then some points would be moot etc)

However, when we arrived at the examination room, neither the two black drives nor the MacBook were prepared or available for review, despite being expressly identified in our motion and probed at the hearing. This raises the question: Why were they not ready unless the Government was already aware of an issue with these items?

B. Refusal of Requested Procedures

The US Attorney categorically refused to allow any examination procedures other than a basic review in FTK Imager during the meeting. Specifically, the US Attorney refused to examine the black hard drives that were the primary focus of our motion and subject of our spoliation claims. He said he's only doing it his way. (Simple health checks or the proof of old forensic images, would have been good too, see exhibit 1,2,3 here as example of verifying drive status)

C. Agent Fell & Coleman Responses and Consciousness of Guilt Implications

When I clearly stated that the presented passwords were incorrect, Agent Fell responded with a raised voice: "Well then we have a problem."

During my review of documents while Agent Fell examined disk drives, it was revealed that some materials were not encrypted. Agent Coleman then stated: "Maybe they had a lot going on" - representing a continued pattern of consciousness of guilt.

Seth Aikens

VIII. AVAILABLE ACCESS METHODS IGNORED BY Government

Despite claims of inability to access encrypted data, the Government had multiple readily available methods that required no cooperation from me:

1. **System Already Logged In:** The computer was operational with full system access at time of seizure
2. **Physical Password Documentation:** Credential papers were present and seized with binder & USB
3. **RAM Dump Capability:** Easy to login with credentials and dump
4. **Standard Forensic Procedures:** Proper imaging could have preserved evidence integrity
5. **Missing USB:** The seized USB device contained additional access credentials **In plain text**

IX. PATTERN OF INVESTIGATIVE MISCONDUCT

The Government's approach raises serious questions about:

1. Whether technical limitations are being deliberately misconstrued as obstruction
2. Whether standard encryption practices are being portrayed as evidence of criminal intent
3. Whether the Government's technical incompetence is being used to justify claims of non-cooperation
4. Whether evidence has been damaged through improper handling and lack of forensic protocols
5. Whether the Government deliberately ignored readily available access methods
6. Whether the complete absence of forensic images represents deliberate evidence destruction

A. Technical Reality of Password Access

Without physical access to the silver binder papers (Or USB/Ram Dump) containing documented passwords, and given their non-constructive, cryptographically secure nature, it is technically

Seth Aikens

impossible for me or anyone else to reproduce, recall, or reconstruct these passwords through memory or computational methods.

B. Government's Alternative Options

However, the Government possessed multiple technical methods to access encrypted data without requiring my assistance, all of which they failed to utilize despite having immediate access at the time of seizure.

C. Critical Issues Requiring Court Intervention

1. **Evidence Preservation Failures:** Complete absence of forensic images has resulted in potential evidence corruption and loss
2. **Missing Evidence:** USB device missing from inventory without forensic preservation
3. **Technical Incompetence:** Agent Coleman's use of obsolete TrueCrypt proves lack of basic forensic examination
4. **Undisclosed Methodology:** Government's failure to reveal "cracking process" or prove use of write blockers and iPhone exams (**When they had the passwords for the phones too!**)
5. **Examination Refusal:** Government's refusal to examine specifically requested evidence
6. **Time-Related Corruption:** Potential evidence degradation due to improper storage and lack of immediate forensic preservation
7. **Alternative Access Failure:** Government's failure to utilize readily available technical access methods present at time of seizure

C. Debunking Baseless Killswitch Claims

As part of my comprehensive technical demonstration, Exhibit 131.9 video includes a detailed segment toward the end specifically addressing and debunking the Government's baseless "killswitch" allegations. This segment provides clear technical evidence demonstrating why such claims are both technically unfounded and logically inconsistent with standard encryption practices.

Seth Aikens

Technical Reality of Encryption Systems

The video demonstration conclusively establishes that the encryption systems utilized in this matter - specifically Cryptomator for cloud-based encryption and VeraCrypt for local encryption - do not contain, support, or enable any form of "killswitch" functionality. These are industry-standard, open-source encryption platforms that operate on fundamental cryptographic principles..

The demonstration illustrates how encryption containers function as passive storage systems that require active user authentication to access contents. There exists no mechanism within these systems for remote activation, data destruction, or external manipulation. The video clearly shows the step-by-step process of container creation, mounting, file storage, and unmounting, demonstrating the absence of any automated or remote destruction capabilities.

Government's Technical Misunderstanding

The killswitch allegations appear to stem from a fundamental misunderstanding of how encryption technology operates. The video demonstration addresses this misconception by showing that:

1. **Encryption containers are passive storage:** They cannot execute commands or respond to remote signals
2. **Access requires explicit user action:** No automated processes can trigger data destruction
3. **Open-source verification:** The encryption software's source code is publicly available and extensively reviewed by security experts worldwide
4. **Standard forensic procedures apply:** Proper imaging and preservation techniques work identically to any other digital storage

X. IPHONE ANOMALIES AND Government'S DEMONSTRABLY FALSE E01 IMAGING CLAIMS

Seth Aikens

A. Unexplained iPhone Anomalies and Government Silence

When we initially identified that the iPhone exhibited clear technical anomalies, the Government has provided absolutely no explanation to this day for these irregularities. These anomalies are not minor technical discrepancies - they represent fundamental inconsistencies in the device's forensic state that any competent digital examiner should be able to explain.

The Government's complete silence regarding these anomalies speaks volumes about either their technical incompetence or their deliberate concealment. A forensically sound examination would document and explain every anomaly encountered during the investigation process.

The papers listing passwords and USB/Logged in PC, all had the iPhone passcodes. Why "crack" them?

B. Government's Categorically False Claims About E01 Image Creation

The Government has made demonstrably false representations to this Court regarding the impossibility of creating E01 forensic images and has had the audacity to suggest that technical corrections to their misinformation constitute "misleading the reader." This is not only technically incorrect but represents a pattern of misrepresentation that undermines their entire digital forensics claims.

See exhibits 1,2,3

C. Technical Reality: Mobile Forensic Tool to E01 Conversion Process

To be absolutely clear, we never claimed that mobile devices should be extracted directly to E01 format during initial acquisition, nor is such a claim present anywhere in our motion. What we have demonstrated is the technical capability to convert existing mobile forensic extraction files from tools like Cellebrite or the like (Greykey, etc.) into E01 forensic image format for proper forensic analysis and verification.

Seth Aikens

The Government has consistently mischaracterized our technical position. The actual technical process involves taking the proprietary extraction files from mobile forensic tools like Cellebrite, Greykey, or similar platforms that the Government claims to possess and converting those files into industry-standard E01 format. This conversion process is not only technically feasible but represents standard forensic practice for ensuring data integrity and enabling independent verification.

D. Standard Forensic Conversion Procedures

Converting mobile forensic extraction data from tools like Cellebrite or the like (Greykey, etc.) to E01 format is fundamental forensic procedure that allows for:

Standardized Analysis: E01 format is universally recognized across forensic platforms, unlike proprietary formats from Cellebrite, Greykey, or similar tools that require specific software licensing and may contain built-in limitations or biases.

Independent Verification: E01 images can be verified by any qualified forensic examiner using any standard forensic toolkit, whereas proprietary files from Cellebrite or the like (Greykey, etc.) often require expensive proprietary software that limits independent analysis.

Data Integrity Confirmation: E01 format includes comprehensive hash verification and integrity checking that ensures the converted data maintains forensic soundness and chain of custody requirements.

Cross-Platform Compatibility: Unlike proprietary formats from Cellebrite or the like (Greykey, etc.), E01 images can be analyzed using multiple forensic platforms, enabling thorough independent examination without vendor lock-in restrictions.

E. Demonstration Video Evidence

Exhibits 1,2,3 shows a specific partial Cellebrite example of this conversion process, proving definitively that mobile forensic extraction data can be successfully converted to E01 format using standard forensic procedures. This evidence directly contradicts the Government's false

Seth Aikens

claims about technical impossibility and demonstrates that their assertions are categorically incorrect.

F. Government's Technical Misrepresentation Pattern

The Government's false claims about E01 imaging impossibility appear designed to prevent independent forensic verification of their extraction procedures using tools like Cellebrite or the like (Greykey, etc.). By claiming that proper forensic imaging cannot be performed, they seek to insulate their forensic work from the technical scrutiny that proper forensic protocols demand.

This misrepresentation serves the Government's litigation interests by:

Preventing Independent Analysis: By falsely claiming technical impossibility, they avoid having to provide data in formats that would allow independent forensic verification of their procedures and conclusions from their Cellebrite, Greykey, or similar tool extractions.

Avoiding Standard Verification: E01 format would enable independent verification of their extraction completeness, data integrity, and procedural compliance from their mobile forensic tools - verification they appear determined to prevent.

Concealing Procedural Deficiencies: Converting to standard forensic format would reveal whether their extraction procedures using Cellebrite or the like (Greykey, etc.) followed proper forensic protocols or contained significant procedural violations.

Limiting Expert Review: Proprietary formats from mobile forensic tools limit which experts can effectively analyze the data, whereas E01 format enables any qualified forensic examiner to conduct independent analysis.

G. Government's "Misleading the Reader" Allegations Are Projection

The Government's accusation that technical corrections constitute "misleading the reader" is pure projection. The only entity misleading anyone is the Government itself through its systematic misrepresentation of basic technical conversion capabilities from mobile forensic platforms.

Seth Aikens

Technical facts about data format conversion from tools like Cellebrite or the like (Greykey, etc.) are not "misleading" - they are corrective responses to the Government's false technical representations. When the Government claims that standard forensic procedures are impossible, providing accurate technical information becomes essential for ensuring this Court receives factual rather than fabricated technical information.

H. Demand for Technical Accountability

The Government must explain their specific technical basis for claiming that mobile forensic tool-to-E01 conversion from platforms like Cellebrite or the like (Greykey, etc.) is impossible when this represents standard forensic procedure performed routinely by digital forensic examiners worldwide. Their systematic pattern of technical misrepresentation should be subject to independent technical verification and appropriate sanctions.

The Court should not accept the Government's convenient technical impossibility claims without demanding specific technical documentation proving their assertions, particularly when those assertions contradict established forensic science and industry-standard procedures for converting data from mobile forensic platforms like Cellebrite, Greykey, and similar tools.

I. Government's Rule 41 Non-Compliance: Forensic Backup Failures Are Not Defendant's Burden

The Government's failure to create forensically sound backups in compliance with Federal Rule of Criminal Procedure 41 represents their own procedural violation, not a burden that can be shifted to the defense. Rule 41 explicitly requires that digital evidence be handled with appropriate safeguards to preserve its integrity and ensure proper chain of custody.

If the Government chose not to create proper forensic backups from their Cellebrite, Greykey, or similar mobile forensic tool extractions, that represents their willful non-compliance with established legal requirements. The defense cannot be held responsible for the Government's decision to ignore fundamental forensic protocols mandated by Rule 41.

Seth Aikens

The Government's apparent position that they can conduct substandard forensic procedures and then claim technical impossibility when asked to provide proper forensic documentation directly contradicts their Rule 41 obligations. These obligations include maintaining the integrity of digital evidence through proper imaging and backup procedures that enable independent verification.

Their failure to maintain forensically sound backups that could be converted to standard E01 format for independent analysis represents a systematic violation of Rule 41's requirements for proper digital evidence handling. The defense should not bear any burden for the Government's deliberate choice to conduct forensically deficient procedures that prevent proper verification and analysis of the digital evidence they claim to possess.

The Court should recognize that Rule 41 compliance is the Government's responsibility, and their failure to maintain proper forensic standards cannot be used as justification for denying the defense access to properly formatted forensic evidence. If the Government cannot provide forensically sound evidence in standard formats due to their own procedural failures, the appropriate remedy is exclusion of that evidence, not acceptance of substandard forensic work that violates established legal and technical requirements.

XI. Government'S MISAPPLICATION OF LEGAL PRECEDENT AND CONSTITUTIONAL STANDARDS

A. Government's Fundamental Misunderstanding of Trombetta

The Government's reliance on *California v. Trombetta*, reveals either profound misunderstanding or deliberate misrepresentation of Supreme Court precedent.

What *Trombetta* Actually Held:

In *Trombetta*, the Supreme Court established a two-part test for when failure to preserve evidence violates due process:

Seth Aikens

1. The evidence must possess "an exculpatory value that was apparent before the evidence was destroyed"
2. The defendant must be "unable to obtain comparable evidence by other reasonably available means"

California v. Trombetta, 467 U.S. 479, 489 (1984).

Critically, *Trombetta* involved:

- Breath samples that were **actually tested**
- Results that were **preserved and provided** to defendants
- Standard procedures **followed properly**
- **Good faith** compliance with protocols, where "the officers here were acting 'in good faith and in accord with their normal practice'" *Id.* at 488

How This Case Differs:

Factor	<i>Trombetta</i>	This Case
Evidence Tested?	Yes - Intoxilyzer results obtained	No - Devices never accessed
Results Preserved?	Yes - Test results provided	No - All access destroyed
Procedures Followed?	Yes - Standard protocol	No - FLETC training violated and lost evidence or destroyed
Good Faith?	Yes - Normal practice	No - Selective destruction
Alternative Evidence?	Yes - Multiple methods	No - Encrypted data unique

Seth Aikens

The Government's attempt to shoehorn this case into *Trombetta* fails because they never obtained any results to preserve--they destroyed the evidence in its entirety. As the Court noted in *Trombetta*, "the evidence to be presented at trial was not the breath itself, but rather the Intoxilyzer results obtained from the breath samples." *Id.* at 487-488. Here, there are no "results" because the Government systematically destroyed all means of obtaining results.

B. The Government Misapplies the *Cooper* Line of Cases

The Government completely ignores *United States v. Cooper*, 983 F.2d 928 (9th Cir. 1993), which provides the directly applicable framework for this exact type of evidence destruction.

The *Cooper* Standard:

In *Cooper*, the Ninth Circuit ordered dismissal where:

1. Laboratory equipment was destroyed that could prove inability to manufacture methamphetamine
2. The equipment's exculpatory value was apparent
3. No comparable evidence existed
4. The Government acted in bad faith

The court emphasized the severity of the remedy: "Because of the Government's bad faith actions, the laboratory equipment seized from Apotheosis Research lies broken and buried in a toxic waste dump...The appropriate remedy is dismissal of the indictment." *United States v. Cooper*, 983 F.2d 928, 930 (9th Cir. 1993).

This Case Exceeds *Cooper* in Every Material Respect:

Cooper Factor

Cooper Case

This Case

Seth Aikens

Government Control	Had laboratory equipment	Had devices + passwords + logged-in system
Exculpatory Value	Could disprove manufacturing capability	Would prove actual innocence
Bad Faith	Destroyed despite preservation requests	Destroyed/Lost + 26-month active deception
Alternative Evidence	None available for manufacturing test	None - encrypted data unique
Physical Destruction	Equipment in toxic waste dump	Binder/Hard drive missing + USB vanished

Cooper established that when the Government destroys evidence with apparent exculpatory value in bad faith, dismissal is the appropriate remedy.

Let's dig even deeper... The record unmistakably demonstrates that work was performed. Yet, how does the Government reconcile this fact with its catalogue of inconsistent statements and shifting narratives? What explanation is there for the repeated contradictions--were they mistakes, or something more deliberate? The Government's responses have evolved from outright denial to grudging acknowledgment, each iteration more damaging to its credibility than the last. When confronted with documentary evidence, the Government has offered explanations that strain credulity and insult the intelligence of this Court.

These are not isolated incidents or mere oversights. The pattern reveals a systematic approach to concealment that began at the investigation's inception and continued through discovery, motion practice, and even into these proceedings. The Government's litigation strategy appears predicated on the assumption that evidence could be hidden, explanations could be fabricated,

Seth Aikens

and the defense could be kept in the dark indefinitely. This represents a fundamental breach of the adversarial system's basic premise: that justice emerges from a fair contest between prepared advocates operating with access to the same essential facts.

Agent Fell's role in these events demands particular scrutiny. What was Agent Fell's involvement in the destruction, loss or concealment of evidence? We know that specifically the audio recordings in the record reveal Scott Andrus [1] and Scott Raybuck [Grand Jury Presentation], knew work was done and were satisfied right after speaking with the Agents [1]. Was he complicit in the fabrication of documents or the misrepresentation of the investigation's status with digital devices? Was it just to inflame? Did he actively participate in misleading the defense and the court? The Government's failure to provide clear answers about Agent Fell's conduct and others is itself telling. His silence, whether imposed or voluntary, speaks volumes about the Government's willingness to shield its agents from accountability even when their actions have compromised the integrity of these proceedings.

The evidence suggests Agent Fell was not merely present during these events but played an active role in shaping the investigation's direction and determining what evidence would be preserved or destroyed. As factual matter, the discovery was his CD as the attached exhibits show, yet his name is conspicuously absent from the Government's explanations of what went wrong and what's up with all the lies. This selective amnesia cannot be coincidental. When Agent Fell's participation becomes inconvenient to the Government's narrative, he simply disappears from their account--a literary device that might work in fiction but has no place in a court of law. Did Agent fell authorize the powerdown?

These are not minor procedural questions, but go to the heart of the integrity of these proceedings. The Government's conduct strikes at the foundation of our criminal justice system: the principle that prosecution must be conducted fairly, with respect for the defendant's rights, and in accordance with clearly established legal standards. When the Government systematically violates these principles, it does more than prejudice a single defendant--it undermines public confidence in the rule of law itself.

Seth Aikens

The Brady doctrine exists precisely because the Government's superior resources and investigative powers create an inherent imbalance that can only be corrected through strict adherence to disclosure obligations. When the Government flouts these obligations, it transforms its natural advantages into instruments of oppression. The prosecutor's duty to seek justice, not merely convictions, becomes an empty platitude when evidence is concealed, destroyed, or misrepresented.

Moreover, the Government's conduct here reveals a troubling institutional attitude: that compliance with discovery obligations is optional, that explanations need only be plausible rather than truthful, and that accountability can be avoided through strategic silence and selective memory. This attitude poisons the well of justice and makes fair resolution impossible.

Given the gravity and clarity of the evidence, can the Government credibly claim anything other than bad faith? Here, the Government's conduct exceeds even that threshold. The systematic nature of the violations, the implausible explanations offered, and the persistent refusal to provide complete and honest accounts all point toward intentional misconduct.

When the record so plainly establishes *prima facie* misconduct and irrefutable proof of work performed, what justification exists for continued governmental obfuscation? The Government's pattern of behavior demonstrates a calculated disregard for its constitutional and ethical obligations. (Non disclosure of signoff sheets, initial "Plea" offer cuts out ZuRI entirely) Each violation built upon the last, creating a web of deception that now ensnares the entire prosecution. The Government cannot credibly claim surprise at these revelations when its own agents were the architects of this misconduct.

The court must ask: if this conduct does not constitute bad faith, what possibly could? If systematic evidence destruction, fabricated explanations, and persistent deception are insufficient to establish bad faith, then the standard becomes meaningless. Courts cannot permit the Government to benefit from its own wrongdoing by setting an impossibly high bar for proving misconduct. Justice requires that deliberate violations of discovery obligations carry real consequences.

Seth Aikens

And if the remedy here is not dismissal, what message does that send about the rule of law and the Government's obligations under Rule 41, Brady, Rule 16 and the like? Lesser sanctions would signal that the Government can violate its most fundamental obligations with impunity, suffering no meaningful consequences for conduct that corrupts the truth-seeking function of our adversarial system. Such a result would encourage similar misconduct in future cases and erode the constitutional protections that safeguard every defendant's right to a fair trial.

The remedy must match the magnitude of the violation. When the Government's misconduct is systematic, deliberate, and prejudicial, only dismissal can restore the integrity that has been lost and deter similar violations in the future.

Cooper's Application to Digital Evidence:

The *Cooper* principle applies with particular force to digital evidence because:

- Encrypted containers are unique and irreplaceable once access is destroyed
- Unlike physical evidence, digital evidence can be perfectly preserved without degradation
- The Government had multiple non-destructive access methods available
- Modern forensic protocols specifically prohibit the type of destructive conduct that occurred here

Accordingly, I respectfully provide the following explanations for each of the attached exhibits and videos. Each exhibit has been included to illustrate and clarify matters of this case, offering the Court a clearer view.

Exhibit 1 → Making an e01 Image part 1

Exhibit 2 → Making an e01 Image part 2

Seth Aikens

Exhibit 3 → Making an e01 Image part 3

Exhibit 4 → Picture fo Magnet Axiom Importing an E01

Exhibit 5 → Example of Random Data Loss Veracrypt

Exhibit 6 → Example of Random Data Loss Veracrypt

Exhibit 7 → Example of Random Data Loss Veracrypt

Exhibit 8 → Example of Random Data Loss Veracrypt

Exhibit 9 → Veracrypt Docs Discussing Corruption

Exhibit 10 → Example of Random Data Loss Veracrypt

Exhibit 11 → Example of Random Data Loss Cryptomator

Exhibit 12 → Example of Random Data Loss Cryptomator

Exhibit 13 → Example of Random Data Loss Cryptomator

Exhibit 14 → Example of Random Data Loss Cryptomator

Exhibit 15 → Example of Random Data Loss Cryptomator

Exhibit 16 → Example of Random Data Loss Cryptomator

Exhibit 17 → Example of Random Data Loss Cryptomator

Exhibit 18 → Picture of Tools Coleman Brought to Meeting, FTK Imager & TrueCrypt

Exhibit 19 → Proof Cryptomator is More for Cloud Storage

Exhibit 20 → Example of Greykey, see “Download” and refer to my E01/Cellebrite Explainer

Exhibit 1,2,3 & Encryption-Explainer.mp4

Seth Aikens

Exhibit 21 → Picture of BruteCam v2 iOS

Exhibit 22 → Picture of BruteCam v2 Android

Exhibit 23 → Picture of Pike Pizza, Ryan's Girlfriends Brothers Pizza Shop App & Menu I Made. (Website too.)

Exhibit 24 → Proof I was a MNVO Reseller (Sim usage in Ryan/Erick projects for cell connection)

Exhibit 25 → Picture of Owl Apps Shirts

Exhibit 26 → Picture of Macbook That's Missing Hardrive being used in 2016 to code

Exhibit 27 → Picture of Macbook That's Missing Hardrive being used in 2015 to code

Exhibit 28 → App Built on the Macbook Missing Hard Drive (Reference the Video How_To_Parse.mp4)

Exhibit 29 → Business Partners in NY/NYC/NJ. I built JMG (JetSet Management's Website in 2015)

Exhibit 30 → Picture of Macbook That's Missing Hardrive being used in 2015 to the Right & Game I Built

Exhibit 31 → Proof I was fine with Police

Exhibit 32 → Picture of Macbook That's Missing Hardrive being used in 2015 to code

Exhibit 33 → Band website I built in 2015.

Exhibit 34 → App I built on my macbook in 2015.

Exhibit 35 → Proof of the TabTap Game x2 Devices in 2015

Seth Aikens

Exhibit 36 → Proof of UPMC Interest In Me

Exhibit 37 → Proof of UPMC Interest In Me

Exhibit 38 → Picture of MacBook that's missing hard drive being used in 2015 to build/run robotics/monitor at the robotics event.

Exhibit 39 → Additional programming pictures from 2015, macbook missing drive left side

Exhibit 40 → Picture of me with a C++ book in 2013....

Exhibit 41 → Picture of when I held a job with Sales Huddle (My parents signed the contract)

Exhibit 42 → Additional proof of programming work 2013.

Exhibit 43 → Picture of Rackspace sending me free gear in 2013 for using their services.

Exhibit 44 → Example of a mockup I did in 2013 and the mac osx hooked up to HDMI with the macbook missing hard drive

Exhibit 45 → Picture of a grant I worked on for our electronics club in school in 2014

Exhibit 46 → Example of other products I've mocked up and built in 2014.

Exhibit 47 → Example of coding in 2014.

Exhibit 48 → Example of Virtual Reality Headset I made in 2014.

Exhibit 49 → Picture of my teacher who would discuss "Big Ideas" with me... The same one who got me into electronics, building physical products (Robots first...) and 3D Printer

Exhibit 50 → Example of coding in 2014.

Exhibit 51 → Example of coding in 2014.

Exhibit 52 → Example of a Game Live on App Store in 2015.

Seth Aikens

Exhibit 53 → Picture of Keen.io sending me free gear in 2015 for using their services.

Exhibit 54 → Example of coding in 2015

Exhibit 55 → Picture of my teacher who would discuss “Big Ideas” with me... The same one who got me into electronics, building physical products (Robots first...) and 3D Printer

Exhibit 56 → Picture of the Macbook now missing the hard drive.

Exhibit 57 → Silver Binder 1 Broken Clasp

Exhibit 58 → Silver Binder 2

Exhibit 59 → An example of the Government misrepresenting drive status. It appears empty. Where is the place to type a password the AUSA said????????

Exhibit 60 → An example of the Government misrepresenting drive status. It appears empty. Where is the place to type a password the AUSA said????????

Exhibit 61 → An example of the Government misrepresenting drive status. It appears empty. Where is the place to type a password the AUSA said????????

Exhibit 62 → An example of the Government misrepresenting drive status. It appears empty. Where is the place to type a password the AUSA said????????

Exhibit 63 → Picture of the Drives we actually plugged in. Notice how the Government didn't want to examine the black drives??? The 2 in safe pictures???

Exhibit 64 → Picture of a different setup then when L/E came in 2022.

Exhibit 65 → Picture of a different setup then when L/E came in 2022.

Exhibit 66 → Picture of a different setup then when L/E came in 2022.

Exhibit 67 → Proof Sales Huddle Group grew into more millions.

Seth Aikens

Exhibit 68 → Proof Sales Huddle Group grew into more millions.

Exhibit 69 → Proof Sales Huddle Group grew into more millions.

Exhibit 70 → BruteCam iOS v1 (In the video I made for your Honor I reference this and v2)

Exhibit 71 → Proof I kept my paperwork in check.

Exhibit 72 → Proof of again 3D Design/print skills.

Exhibit 73 → Picture of Craig e911 Signoff Digitally

Exhibit 74 → Tangible Evidence Indicates the Missing MacBook Contained Exculpatory Information, Dismissing Any Claims of "Speculation."

Exhibit 75 → Proof of a Website done in 2020.

Exhibit 76 → An example of Erick Merryman's Loader Serco can be seen here. If you look at the top bar of the loader, you'll notice a light; this is part of the project's placement, indicating where my lights would be installed.

Exhibit 77 → Breach of Contract Notice + NOTICE TO PRESERVE (Marco never turned over that to Federal Investigators!) P1

Exhibit 78 → Breach of Contract Notice + NOTICE TO PRESERVE (Marco never turned over that to Federal Investigators!) P2

Exhibit 79 → Breach of Contract Notice + NOTICE TO PRESERVE (Marco never turned over that to Federal Investigators!) P3

Exhibit 80 → Breach of Contract Notice + NOTICE TO PRESERVE (Marco never turned over that to Federal Investigators!) P4

Seth Aikens

Exhibit 81 → Picture of a similar supplier that I used to order equipment. If Raybuck can like/interact with these companies, why couldn't I set up/do something similar!? Notice why we would need the avaresupply emails!

Exhibit 82 → An example of Erick Merryman's Back Log Bunk can be seen here. If you look left above mud flaps and right, you'll notice a light; this is part of the project's placement, indicating where my lights would be installed. They also go horizontal on the bunk racks (tall up out of view slightly)

Exhibit 83 → Proof the Non Drive Missing Macbook in Exhibit 119 Contains Exculpatory Info too. Wouldn't a jury maybe want to see other projects?

Exhibit 84 → Proof the Non Drive Missing Macbook in Exhibit 119 Contains Exculpatory Info too. Wouldn't a jury maybe want to see other projects?

Exhibit 85 → Proof I helped during covid; crowdsource covid shorted supplies.

Exhibit 86 → Picture of the text anomalies with Erick Merryman's Wife Ronna

Exhibit 87 → An example of Erick Merryman's entire truck. If you look left above mud flaps and right, you'll notice a light; this is part of the project's placement, indicating where my lights would be installed. They also go horizontal on the bunk racks (In view now)

Exhibit 88 → Proof that the missing Initial Versions for Click To Reserve, we're missing is indeed ****real****.

Exhibit 89 → Proof I helped during covid; setup a covid finder website.

Exhibit 90 → Proof of my ****Industrial**** like 3D Printers. Before this, I owned a similar one going way back.

Exhibit 91 → Brute Cam v2 iOS.

Seth Aikens

Exhibit 92 → Proof of a ZuRI Scanner phone with IMEI. Is there a Government subpoena involved? No...

Exhibit 93 → Brute Cam v2 Web (Discussed for your Honor in the Trail Cam Vid)

Exhibit 94 → Brute Cam v2 Web (Discussed for your Honor in the Trail Cam Vid)

Exhibit 95 → Proof Craig e911 had spent since 2016 working on his App Idea, I BUILT...

Exhibit 96 → Proof of a Logo Design in 2020.

Exhibit 97 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 98 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 99 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 100 → Image of the Government's findings, including just subpoenas and some documents. It's nothing compared to what we've submitted for the record.

Exhibit 101 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 102 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 103 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 104 → Picture of an ACTUAL computer withOUT hard drive the Government DIDN'T take.

Seth Aikens

Exhibit 105 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 106 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 107 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 108 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 109 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 110 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 111 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 112 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 113 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 114 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 115 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Seth Aikens

Exhibit 116 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 117 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 118 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 119 → Picture of my other ****NEW**** macbook, reference exhibit Exhibit 74. I barely got a few projects on this one versus my 2011 that went back YEARS...

Exhibit 120 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 121 → Proof the Exhibit 74 has exculpatory info on the android phone... Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 122 → Proof of Labels Government seized

Exhibit 123 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 124 → Government Photos. Doesn't support the Government's assertion of papers vs binder. No papers with passwords anywhere.

Exhibit 125 → Government Search Warrant Return Log. No proper narrow categorizing, just general. Doesn't support the Government's assertion of papers vs binder.

Exhibit 126 → Government Search Warrant Return Log. No proper narrow categorizing, just general. Doesn't support the Government's assertion of papers vs binder.

Seth Aikens

Exhibit 127 → Government Search Warrant Return Log. No proper narrow categorizing, just general. Doesn't support the Government's assertion of papers vs binder.

Exhibit 128 → Government Search Warrant Return Log. No proper narrow categorizing, just general. Doesn't support the Government's assertion of papers vs binder.

Exhibit 129 → Government Search Warrant Return Log. No proper narrow categorizing, just general. Doesn't support the Government's assertion of papers vs binder.

Exhibit 130 → I've been working on the TroeseLaw.com website for several years. I'm puzzled as to why the Government hasn't recognized that as legitimate work and acknowledged the same exculpatory knowledge. The agent's warrant affidavit mentions researching his identity. I also manage the Google My Business account. So, what's going on?

Exhibits 131.1 through 132.7 are videos playable via the link. Last Visited All Aug 5th 2025.

Praying and submitting respectfully that the Court should reject the Government's proposed findings and conclusions.

Thank you for your consideration.

Respectfully submitted

/s/ Seth Allen Aikens II

Defendant

